REMARKS

The Office Action of October 13, 2009 has been received and its contents carefully considered.

The Office Action rejects all of the claims for obviousness based on a published US application by Felsher (which incorporates by reference a large number of other items of prior art) in view of a published US application by Tello. The rejection is respectfully traversed.

Claim 1 provides that an authorization module includes "a password fingerprint unit, an environment fingerprint sampling unit, and a time fingerprint sampling unit, which are set in parallel ...". The Office Action takes the position that such an authorization module is disposed in Felsher's paragraphs [0087] and [0354].

Felsher's paragraph [0087] summarizes the disclosure of one of the many items of prior art that Felsher incorporates by reference. Paragraph [0087] says that, in one embodiment of the prior art item, "verification includes locking the digital information to the requesting computer system by comparing a generated digital fingerprint associated with the digital information to a digital fingerprint previously generated which is unique to the requesting computer system."

Felsher's paragraph [0354] advises that the authenticity of a user

> ...may be verified with a hardware token, such as the RSA SecurID hardware token. These tokens are small, handheld devices containing microprocessors that calculate and display unpredictable codes. These codes change at a specified interval, typically 60 seconds.

Felsher's paragraph [0354] goes on to say that the user enters the password that is currently displayed on the SecurID device and, if the password that the user enters does not match what is currently being displayed, the password from the previous sixty second interval is also checked in case there was a delay in typing and transmission.

It is respectfully submitted that Felsher neither discloses nor suggests an authorization module that includes a password fingerprint unit, an environment fingerprint sampling unit and a time fingerprint sampling unit. One reason for this assertion is that Felsher would not have led an ordinarily skilled person to think that the technique disclosed in the item of prior art discussed in paragraph [0087] is used in combination with the RSA SecurID system

described in paragraph [0354]. Another reason is that claim 1 provides that the password fingerprint unit, the environment fingerprint sampling unit and the time fingerprint sampling unit are "set in parallel." It is difficult to envision how an RSA SecurID hardware token could be included in the same authorization module as the other units of the authorization module that are specified in claim 1, much less how the RSA SecurID hardware token could be "set in parallel" with the other units.

Additionally, the fact that the RSA SecurID password displayed on the hardware token is valid for only a certain time period does not make it a "time fingerprint sampling unit." Just what is it that is sampled? Certainly not a time fingerprint.

The present application discloses an access authorization system that includes an environment fingerprint sampling unit, and an administrator can designate one or more valid authorization environments based on practical needs. The environment fingerprint sampling unit provides unique and unduplicatable data to be used as the fingerprint of the environment. This unique and unduplicatable data can be the MAC address of a network card, the serial number of a hard drive, or so forth. The access authorization system also includes a password fingerprint unit and a time fingerprint sampling unit. The password fingerprint unit generates unique and unduplicatable data to be used as the password fingerprint according to a designated password. The time fingerprint sampling unit generates unique and unduplicatable data to be used as the time fingerprint, according to the current time and a time limit designated by the administrator. Thus, once the administrator has designated a valid authorization environment and a valid authorization time period, a user holding a legal password can access a secret file only from an authorized environment and within the authorized time period. Hackers are thwarted because only an authorized user can access a secret file, during an authorized time period and from an authorized environment. Felsher does not suggest this triplex protection, in which a secret file can be accessed only if three kinds of fingerprints are certified.

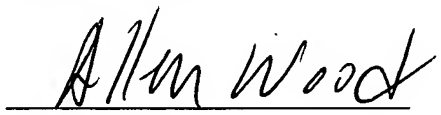
It is also respectfully submitted that the RSA SecurID hardware token mentioned in the Felsher reference cannot function as an environment fingerprint sampling unit and a time fingerprint sampling unit. It is used for providing a two-factor authentication that includes a time component; that is to say, the user must combine his "PIN number" with a token code

(which typically changes every sixty seconds) in order to access a secret file. The token does not collect unique and unduplicatable data from a designated environment. Instead, it generates an unpredictable code every sixty seconds using the same algorithm as an authorization server, regardless of whether or not there is a time limit for accessing a secret file. As long as a user holds a legal token (the user must also have a legal PIN, of course) then each code that token outputs at any time will be the same as the code generated by the authorization server, and the user will be able to access the secret file at any time and from any environment. The token does not generate unique and unduplicatable data according to the current time and a time limit designated by the administrator. It automatically changes periodically (typically every sixty seconds) regardless of whether there is a time limit for accessing a secret file.

For the reasons discussed above, it is respectfully submitted that the invention defined by claim 1 is patentable over the cited references. Since the remaining claims depend from claim 1 and recite additional limitations to further define the invention, they are automatically patentable along with claim 1 and need not be further discussed.

For the foregoing reasons, it is respectfully submitted that this application is in condition for allowance. Reconsideration of the application is therefore respectfully requested.

Respectfully submitted,



Allen Wood
Registration No. 28,134
Rabin & Berdo, P.C.
Customer No. 23995
(202) 326-0222 (telephone)
(202) 408-0924 (facsimile)

AW/ng